Mobile IP Working Group
INTERNET-DRAFT

David B. Johnson
Carnegie Mellon University
Charles Perkins
Sun Microsystems
30 July 1997

Mobility Support in IPv6

<draft-ietf-mobileip-ipv6-03.txt>

Status of This Memo

Abstract

This document specifies the operation of mobile computers using IPv6. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send packets destined for the mobile node directly to it at this care-of address.

INTERNET-DRAFT Mobility Support in IPv6 30 July 1997

Contents

1. Introduction

This document specifies the operation of mobile computers using Internet Protocol Version 6 (IPv6) [5]. Without specific support for mobility in IPv6, packets destined to a mobile node (host or router) would not be able to reach it while the mobile node is away from its home IPv6 subnet, since routing is based on the network prefix in a packet's destination IP address. In order continue communication in spite of its movement, a mobile node could change its IP address

each time it moves to a new IPv6 subnet, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6.

The protocol operation defined here, known as Mobile IPv6, allows a mobile node to move from one IPv6 subnet to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address", the IP address assigned to the mobile node within its home IPv6 subnet. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes (stationary or mobile) after moving to a new subnet. The movement of a mobile node away from its home subnet is thus transparent to transport and higher-layer protocols and applications.

The Mobile IPv6 protocol is just as suitable for mobility across homogeneous media as for mobility across heterogeneous media. For example, Mobile IPv6 facilitates node movement from one Ethernet segment to another as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with the mobile node's IP address remaining unchanged in spite of such movement.

One can think of the Mobile IPv6 protocol as solving the "macro" mobility management problem. More "micro" mobility management applications -- for example, handoff amongst wireless transceivers, each of which covers only a very small geographic area -- are possibly more suited to other solutions. For example, as long as node movement does not occur between link-level points of attachment on different IPv6 subnets, link-layer mobility support offered by a number of current wireless LAN products is likely to offer faster convergence and lower overhead than Mobile IPv6. Extensions to the Mobile IPv6 protocol are also possible to support a more local, hierarchical form of handoff, but such extensions are beyond the sope of this document.

2. Terminology

2.1. General Terms

IP

Internet Protocol Version 6 (IPv6).

node

A device that implements IP.

router

A node that forwards IP packets not explicitly addressed to itself.

host

Any node that is not a router.

link

A communication facility or medium over which nodes can communicate at the link layer, such as an Ethernet (simple or bridged). A link is the layer immediately below IP.

interface

A node's attachment to a link.

network prefix

A bit string that consists of some number of initial bits of an IP address.

link-layer address

A link-layer identifier for an interface, such as IEEE 802 addresses on Ethernet links.

packet

An IP header plus payload.

2.2. Mobile IPv6 Terms

home address

An IP address assigned to a mobile node within its home subnet. The network prefix in a mobile node's home address is equal to the network prefix of the home subnet.

home subnet

The IP subnet indicated by a mobile node's home address. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home subnet.

mobile node

A node that can change its link-level point of attachment from

one IP subnet to another, while still being reachable via its home address.

movement

A change in a mobile node's point of attachment to the Internet such that it is no longer link-level connected to the same IP subnet as it was previously. If a mobile node is not currently link-level connected to its home subnet, the mobile node is said to be "away from home".

correspondent node

A peer node with which a mobile node is communicating. The correspondent node may be either mobile or stationary.

foreign subnet

Any IP subnet other than the mobile node's home subnet.

home agent

A router on a mobile node's home subnet with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home subnet destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

care-of address

An IP address associated with a mobile node while visiting a foreign subnet, which uses the network prefix of that foreign subnet. Among the multiple care-of addresses that a mobile node may have at a time (e.g., with different network prefixes), the one registered with the mobile node's home agent is called its "primary" care-of address.

binding

The association of the home address of a mobile node with a care-of address for that mobile node, along with the remaining lifetime of that association.

2.3. Specification Language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

MUST

This word, or the adjective "REQUIRED", means that the definition is an absolute requirement of the specification.

MUST NOT

This phrase means that the definition is an absolute prohibition of the specification.

SHOULD

This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT

This phrase means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY

This word, or the adjective "OPTIONAL", means that an item is truly optional. For example, one vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product, while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option.

silently discard

The implementation discards the packet without further processing, and without indicating an error to the sender. The implementation SHOULD provide the capability of logging the error, including the contents of the discarded packet, and SHOULD record the event in a statistics counter.

3. Overview of Mobile IPv6 Operation

3.1. Protocol Summary

A mobile node is always addressable by its home address, whether it is currently attached to its home subnet or is away from home. While a mobile node is at home, packets addressed to the mobile node's home address are routed to it using conventional Internet routing mechanisms in the same way as if the node were never mobile. Since the network prefix of a mobile node's home address is equal to the network prefix of its home subnet, packets addressed to it will be routed to its home subnet.

While a mobile node is attached to some foreign subnet away from home, it is also addressable by one or more care-of addresses, in addition to its home address. A care-of address is an IP address associated with a mobile node while visiting a particular foreign subnet. The network prefix of a mobile node's care-of address is equal to the network prefix of the foreign subnet being visited by the mobile node; if the mobile node is link-level connected to this foreign subnet while using that care-of address, packets addressed to this care-of address will be routed to the mobile node in its location away from home. The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. A mobile node typically acquires its care-of address through stateless [16] or stateful (e.g., DHCPv6 [3]) address autoconfiguration, according to the methods of IPv6 Neighbor Discovery [9], although other methods of acquiring a care-of address are also possible.

While away from home, the mobile node registers one of its bindings with a router in its home subnet, requesting this router to function as the "home agent" for the mobile node. This binding registration is done by the mobile node sending a packet with a "Binding Update" destination option to the home agent, which replies by returning a packet containing a "Binding Acknowledgement" destination option to the mobile node. The care-of address in this binding registered with its home agent is known as the mobile node's "primary care-of address". The mobile node's home agent thereafter uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address on the home subnet, and tunnels each intercepted packet to the mobile node's primary care-of address. To tunnel each intercepted packet, the home agent encapsulates the packet using IPv6 encapsulation [4], addressed to the mobile node's primary care-of address.

The Binding Update and Binding Acknowledgement destination options, together with a "Binding Request" destination option, are also used

to allow IPv6 nodes communicating with a mobile node, to dynamically learn and cache the mobile node's binding. When sending a packet to any IPv6 destination, a node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses an IPv6 Routing header [5] (instead of IPv6 encapsulation) to route the packet to the mobile node by way of the care-of address indicated in this binding. If, instead, the sending node has no cached binding for this destination address, the node sends the packet normally (with no Routing header), and the packet is subsequently intercepted and tunneled by the mobile node's home agent as described above. A node communicating with a mobile node is referred to in this document as a "correspondent node" of the mobile node.

Since a Binding Update, Binding Acknowledgement, and Binding Request are each represented in a packet as an IPv6 destination option [5], they may be included in any IPv6 packet. Any of these options can be sent in either of two ways:

- A Binding Update, Binding Acknowledgement, or Binding Request can be included within any IPv6 packet carrying any payload such as TCP [14] or UDP [13].

- A Binding Update, Binding Acknowledgement, or Binding Request can be sent as a separate IPv6 packet containing no payload. In this case, the Next Header field in the Destination Options header is set to the value 59, to indicate "No Next Header" [5].

Mobile IPv6 also defines one additional IPv6 destination option. When a mobile node sends a packet while away from home, it will generally set the Source Address in the packet's IPv6 header to one of its current care-of addresses, and will also include a "Home Address" destination option in the packet, giving the mobile node's

home address. Many routers implement security policies such as "ingress filtering" [6] that do not allow forwarding of packets that appear to have a Source Address that is not topologically correct. By using the care-of address as the IPv6 header Source Address, the packet will be able to pass normally through such routers, yet ingress filtering rules will still be able to locate the true physical source of the packet in the same way as packets from non-mobile nodes. By also including the Home Address option, the sending mobile node can communicate its home address to the correspondent node receiving this packet, allowing the use of the care-of address to be transparent above the Mobile IPv6 support level (e.g., at the transport layer). The inclusion of a Home Address option in a packet affects only the correspondent node's receipt of this single packet; no state is created or modified in the

correspondent node as a result of receiving a Home Address option in a packet.

In summary, the following four new IPv6 destination options are defined for Mobile IPv6:

Binding Update

A Binding Update option is used by a mobile node to notify a correspondent node or the mobile node's home agent of its current binding. The Binding Update sent to the mobile node's home agent to register its primary care-of address is marked as a "home registration". Any packet that includes a Binding Update option MUST also include an IPv6 Authentication header [1], providing sender authentication, data integrity protection, and replay protection. The Binding Update option is described in detail in Section 4.1.

Binding Acknowledgement

A Binding Acknowledgement option is used to acknowledge receipt of a Binding Update, if an acknowledgement was requested in the Binding Update. Any packet that includes a Binding Acknowledgement option MUST also include an IPv6 Authentication header [1], providing sender authentication, data integrity protection, and replay protection. The Binding Acknowledgement option is described in detail in Section 4.2.

Binding Request

A Binding Request option is used to request a mobile node to send a Binding Update to the requesting node, containing the mobile node's current binding. This option is typically used by a correspondent node to refresh a cached binding for a mobile node, when the cached binding is in active use but the binding's lifetime is close to expiration. No special authentication is required for the Binding Request option. The

Binding Request option is described in detail in Section 4.3.

Home Address

A Home Address option is used in a packet sent by a mobile node to inform the recipient of that packet of the mobile node's home address. For packets sent by a mobile node while away from home, the mobile node generally uses one of its care-of addresses as the Source Address in the packet's IPv6 header. By including a Home Address option in the packet, the correspondent node receiving the packet is able to substitute

the mobile node's home address for this care-of address when processing the packet, thus making the use of the care-of address transparent to the correspondent node. The Home Address option is described in detail in Section 4.4.

Extensions to the format of these options may be included after the fixed portion of the option data specified in this document. The presence of such extensions will be indicated by the Option Length field within the option. When the Option Length is greater than the length required for the option specified here, the remaining octets are interpreted as extensions. Currently, no extensions have been defined.

This document describes the Mobile IPv6 protocol in terms of the following two conceptual data structures used in the maintenance of cached bindings:

Binding Cache

A cache, maintained by each IPv6 node, of bindings for other nodes. An entry in a node's binding cache for which the node is serving as a home agent is marked as a "home registration" entry and SHOULD NOT be deleted by the home agent until the expiration of its binding lifetime. Other Binding Cache entries MAY be replaced at any time by any reasonable local cache replacement policy but SHOULD NOT be unnecessarily deleted. Any node's Binding Cache may contain at most one entry for each mobile node, keyed by the mobile node's home address. The contents of a node's Binding Cache MUST NOT be changed in response to a Home Address option in a received packet. The Binding Cache MAY be implemented in any manner consistent with the external behavior described in this document, for example by being combined with the node's Destination Cache as maintained through Neighbor Discovery [9].

Binding Update List

A list, maintained by each mobile node, recording information for each Binding Update sent by this mobile node, for which the Lifetime of the binding sent in that Binding Update has not yet expired. The Binding Update List includes all bindings

sent by the mobile node: those to correspondent nodes, to the mobile node's home agent, and to a previous default router of the mobile node. Each Binding Update List entry records the IP address of the node to which the Update was sent, the home address for which one Binding Update was sent, and the remaining lifetime of that binding. The Binding Update List

MAY be implemented in any manner consistent with the external behavior described in this document.

When a mobile node configures a new care-of address and decides to use this new address as its primary care-of address, the mobile node registers this new binding with its home agent by sending the home agent a Binding Update. The mobile node indicates that an acknowledgement is needed for this Binding Update and continues to periodically retransmit it until acknowledged. The home agent acknowledges the Binding Update by returning a Binding Acknowledgement to the mobile node.

When a mobile node receives a packet tunneled to it from its home agent, the mobile node assumes that the original sending correspondent node has no binding cache entry for the mobile node, since the correspondent node would otherwise have sent the packet directly to the mobile node using a Routing header. The mobile node thus returns a Binding Update to the correspondent node, allowing it to cache the mobile node's binding for routing future packets. Although the mobile node may request an acknowledgement for this Binding Update, it need not, since subsequent packets from the correspondent node will continue to be intercepted and tunneled by the mobile node's home agent, effectively causing any needed Binding Update retransmission.

A correspondent node with a binding cache entry for a mobile node may refresh this binding, for example if the binding's lifetime is near expiration, by sending a Binding Request to the mobile node. Normally, a correspondent node will only refresh a binding cache entry in this way if it is actively communicating with the mobile node and has indications, such as an open TCP connection to the mobile node, that it will continue this communication in the future. When a mobile node receives a Binding Request, it replies by returning a Binding Update to the node sending the Binding Request.

A mobile node may use more than one care-of address at the same time, although only one care-of address may be registered for it at its home agent as its primary care-of address. The mobile node's home agent will tunnel all intercepted packets for the mobile node to its (single) registered primary care-of address, but the mobile node will accept packets that it receives at any of its current care-of addresses. Use of more than one care-of address by a mobile node may be useful, for example, to improve smooth handoff when the mobile node moves from one wireless IP subnet to another. If each wireless subnet is connected to the Internet through a separate base station,

such that the wireless transmission range from the two base stations overlap, the mobile node may be able to remain link-level connected within both subnets while in the area of overlap. In this case, the

mobile node could acquire a new care-of address in the new subnet before moving out of transmission range and link-level disconnecting from the old subnet. The mobile node may thus still accept packets at its old care-of address while it works to update its home agent and correspondent nodes, notifying them of its new care-of address in the new subnet.

Since correspondent nodes cache bindings, it is expected that correspondent nodes usually will route packets directly to the mobile node's care-of address, so that the home agent is rarely involved with packet transmission to the mobile node. This is essential for scalability and reliability, and for minimizing overall network load. By caching the care-of address of a mobile node, optimal routing of packets can be achieved from the correspondent node to the mobile node. Routing packets directly to the mobile node's care-of address also eliminates congestion at the mobile node's home agent and home subnet. In addition, the impact of of any possible failure of the home agent, the home subnet, or intervening networks leading to or from the home subnet is reduced, since these nodes and links are not involved in the delivery of most packets to the mobile node.

3.2. Comparison with Mobile IP for IPv4

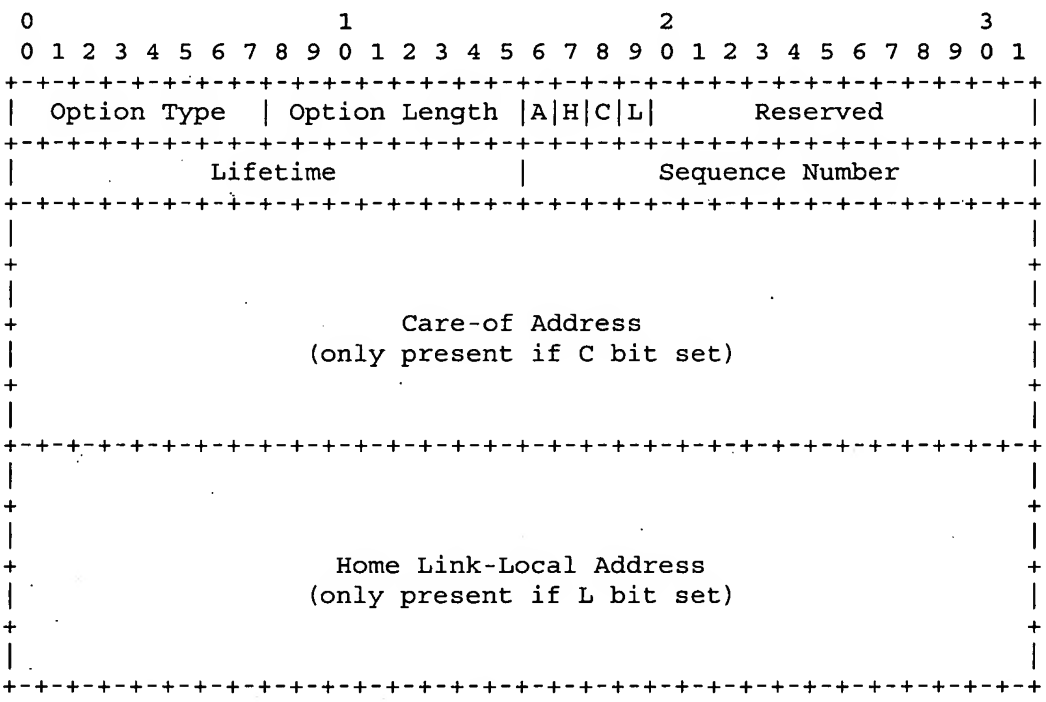
[This section will include a comparison between the Mobile IPv6 protocol and the Mobile IPv4 protocol [11, 10, 12]. However, this comparison has not yet been written. It will be filled in with the next revsion to this draft.]

4. New IPv6 Destination Options

4.1. Binding Update Option

The Binding Update destination option is used by a mobile node to notify a correspondent node or the mobile node's home agent of a new care-of address.

The Binding Update option is encoded in type-length-value (TLV) format as follows:



Option Type

192 ???

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. For the current definition of the Binding Update option, the minimum value for this field is 6, for the case in which neither the Care-of Address Present (C) bit nor the Home Link-Local Address Present (L) bit are set, and the maximum value is 38, for the case in which both of these bits are set.

Acknowledge (A)

The Acknowledge (A) bit is set by the sending node to request a Binding Acknowledgement (Section 4.2) be returned upon receipt of the Binding Update option.

Home Registration (H)

The Home Registration (H) bit is set by the sending node to request the receiving node to act as this node's home agent. The Destination Address in the IP header of the packet carrying this option MUST be that of a router sharing the same network prefix as the home address of the mobile node in the binding (given by the Home Address field in the Home Address option in the packet).

Care-of Address Present (C)

The Care-of Address Present (C) bit indicates the presence of the Care-of Address field in the Binding Update. The care-of address for this binding is either the address in the Care-of Address field in the Binding Update, if this bit is set, or the Source Address in the packet's IPv6 header, if this bit is not set.

Home Link-Local Address Present (L)

The Home Link-Local Address Present (L) bit indicates the presence of the Home Link-Local Address field in the Binding Update. This bit is set by the sending node to request the receiving node to act as a proxy (for participating in the Neighbor Discovery Protocol) for the node while it is away from home. This bit MUST NOT be set unless the Home Registration (H) bit is also set in the Binding Update.

Reserved

Sent as 0; ignored on reception.

Lifetime

16-bit unsigned integer. The number of seconds remaining before the binding must be considered expired. A value of all ones (0xffff) indicates infinity. A value of zero indicates that the Binding Cache entry for the mobile node should be deleted.

INTERNET-DRAFT Mobility Support in IPv6 30 July 1997

Sequence Number

Used by the receiving node to sequence Binding Updates and by the sending node to match a returned Binding Acknowledgement with this Binding Update. Each Binding Update sent by a mobile node MUST use a Sequence Number greater than the Sequence Number value sent in the previous Binding Update (if any) to the same destination address (modulo 2**16). There is no requirement, however, that the Sequence Number value strictly increase by 1 with each new Binding Update sent.

Care-of Address

This field in the Binding Update is optional and is only present when the Care-of Address Present (L) bit is set. If present, it gives the care-of address of the mobile node for this binding. For most Binding Updates sent, it is expected that this field will not be present, and instead that the care-of address for the binding will be given by the Source Address field in the packet's IPv6 header.

Home Link-Local Address

This field in the Binding Update is optional and is only present when the Home Link-Local Address Present (L) bit is set. If present, it gives the link-local address of the mobile node used by the mobile node when it was last attached to its home subnet.

Any packet including a Binding Update option MUST also include a Home Address option. The home address of the mobile node in the binding given in the Binding Update option is indicated by the Home Address field in the Home Address option in the packet.

Any packet that includes a Binding Update option MUST include an IPv6 Authentication header [1] in order to protect against forged Binding Updates. The authentication MUST provide sender authentication, data integrity protection, and replay protection.

If the care-of address in the binding (either the Care-of Address field in the Binding Update option or the Source Address field in the packet's IPv6 header) is equal to the home address of the mobile node, the Binding Update option indicates that any existing binding for the mobile node should be deleted. Likewise, if the Lifetime field in the Binding Update option is equal to 0, the Binding Update option indicates that any existing binding for the mobile node should be deleted. In each of these cases, no Binding Cache entry for the

mobile node should be created in response to receiving the Binding Update.

The three highest-order bits of the Option Type are encoded to indicate specific processing of the option [5]. For the Binding

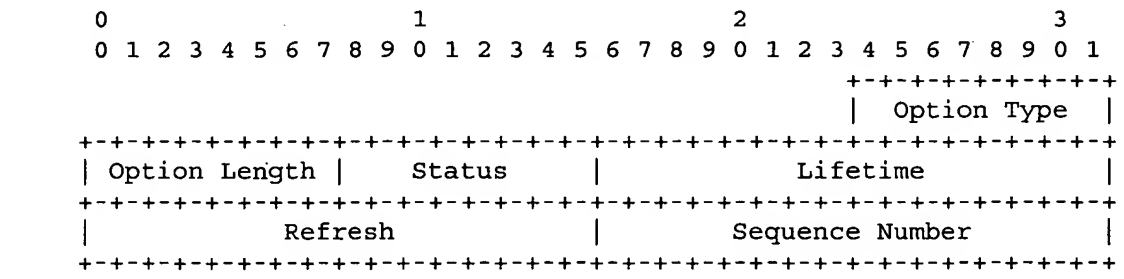
Update option, these three bits are set to 110, indicating that the data within the option cannot change en-route to the packet's final destination, and that any IPv6 node processing this option that does not recognize the Option Type must discard the packet and, only if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address.

Extensions to the Binding Update option format may be included after the fixed portion of the Binding Update option specified above. The presence of such extensions will be indicated by the Option Length field. When the Option Length is greater than the length defined above, depending on the state of the Care-of Address Present (C) and Home Link-Local Address Present (L) bits, the remaining octets are interpreted as extensions. Currently, no extensions have been defined.

4.2. Binding Acknowledgement Option

The Binding Acknowledgement destination option is used to acknowledge receipt of a Binding Update option (Section 4.1). When a node receives a packet containing a Binding Update option, with this node being the destination node of the packet, this node MUST return a Binding Acknowledgement to the source of the packet, if the Acknowledge (A) bit is set in the Binding Update.

The Binding Acknowledgement option is encoded in type-length-value (TLV) format as follows:



Option Type

193 ???

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. For the current definition of the Binding Acknowledgement option, this field MUST be set to 9.

Status

8-bit unsigned integer indicating the disposition of the Binding Update. Values of the Status field less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Binding Update accepted

Values of the Status field greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified
129 Poorly formed Binding Update

130 Administratively prohibited
131 Insufficient resources
132 Home registration not supported
133 Not home subnet
134 Sequence Number field value too small
135 Dynamic home agent address discovery response

Up-to-date values of the Status field are to be specified in the most recent "Assigned Numbers" [15].

Lifetime

The granted lifetime for which this node will attempt to retain

the entry for this mobile node in its binding cache. If the node sending the Binding Acknowledgement is serving as the mobile node's home agent, the Lifetime period also indicates the period for which this node will continue this service; if the mobile node requires home agent service from this node beyond this period, the mobile node MUST send a new Binding Update to it before the expiration of this period, in order to extend the lifetime.

Refresh

The recommended period at which the mobile node SHOULD send a new Binding Update to this node in order to "refresh" the mobile node's binding in this node's binding cache. This refreshing of the binding is useful in case the node fails and loses its cache state. The Refresh period is determined by the node sending the Binding Acknowledgement (the node caching the binding). If this node is serving as the mobile node's home agent, the Refresh value may be set, for example, based on whether the node stores the mobile node's binding in volatile storage or in nonvolatile storage. If the node sending the Binding Acknowledgement is not serving as the mobile node's home agent, the Refresh period SHOULD be set equal to the Lifetime period in the Binding Acknowledgement; even if this node loses this cache entry due to a failure of the node, packets from it can still reach the mobile node through the mobile node's home agent, causing a new Binding Update to this node to allow it to recreate this cache entry.

Sequence Number

The Sequence Number in the Binding Acknowledgement is copied from the Sequence Number field in the Binding Update option, for use by the mobile node in matching this Acknowledgement with an outstanding Binding Update.

Any packet that includes a Binding Acknowledgement option MUST include an IPv6 Authentication header [1] in order to protect against forged Binding Acknowledgements. The authentication MUST provide sender authentication, data integrity protection, and replay protection.

If the node returning the Binding Acknowledgement accepted the Binding Update for which the Acknowledgement is being returned (the value of the Status field in the Acknowledgement is less than 128), this node will have an entry for the mobile node in its Binding Cache, and MUST use this entry (which includes the care-of address received in the Binding Update) in sending the packet containing the Binding Acknowledgement to the mobile node. The details of sending this packet to the mobile node are the same as for sending any packet to a mobile node using a binding, and are described in Section 6.8. The packet is sent using a Routing header, routing the packet to the mobile node by way of its care-of address recorded in the Binding

Cache entry.

If the node returning the Binding Acknowledgement instead rejected the Binding Update (the value of the Status field in the Acknowledgement is greater than or equal to 128), this node MUST similarly use a Routing header in sending the packet containing the Binding Acknowledgement, as described in Section 6.8, but MUST NOT use its Binding Cache in forming the IP header or Routing header in this packet. Rather, the care-of address used by this node in sending the packet containing the Binding Acknowledgement MUST be copied from the care-of address received in the rejected Binding Update; this node MUST NOT modify its Binding Cache in response to receiving this rejected Binding Update and MUST ignore its Binding Cache in sending the packet in which it returns this Binding Acknowledgement. The packet is sent using a Routing header, routing the packet to the home address of the rejected Binding Update by way of the care-of address indicated in the packet containing the Binding Update.

The three highest-order bits of the Option Type are encoded to indicate specific processing of the option [5]. For the Binding Acknowledgement option, these three bits are set to 110, indicating that the data within the option cannot change en-route to the packet's final destination, and that any IPv6 node processing this option that does not recognize the Option Type must discard the packet and, only if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address.

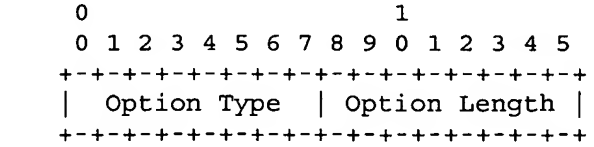
Extensions to the Binding Acknowledgement option format may be included after the fixed portion of the Binding Acknowledgement

option specified above. The presence of such extensions will be indicated by the Option Length field. When the Option Length is greater than 8 octets, the remaining octets are interpreted as extensions. Currently, no extensions have been defined.

4.3. Binding Request Option

The Binding Request destination option is used to request a mobile node's binding from the mobile node. When a mobile node receives a packet containing a Binding Request option, it SHOULD return a Binding Update (Section 4.1) to the source of the Binding Request.

The Binding Request option is encoded in type-length-value (TLV) format as follows:



Option Type

194 ???

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. For the current definition of the Binding Request option, this field

MUST be set to 0.

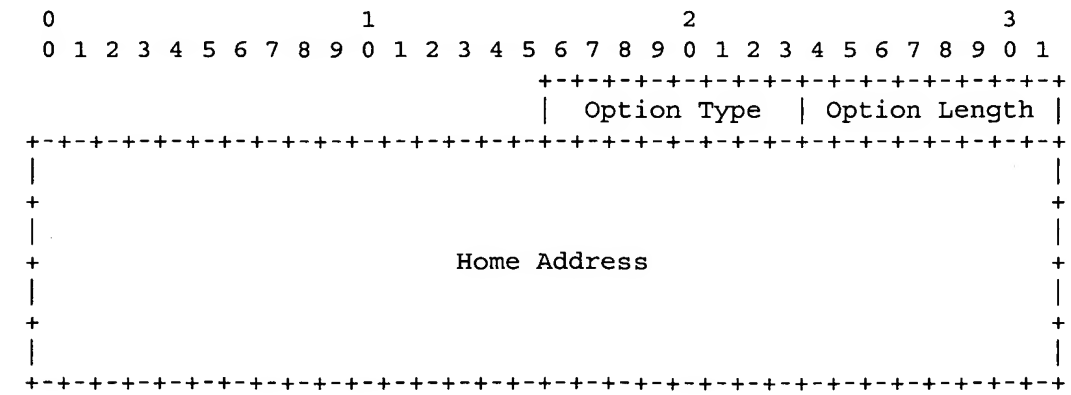
The three highest-order bits of the Option Type are encoded to indicate specific processing of the option [5]. For the Binding Request option, these three bits are set to 110, indicating that the data within the option cannot change en-route to the packet's final destination, and that any IPv6 node processing this option that does not recognize the Option Type must discard the packet and, only if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address.

Extensions to the Binding Request option format may be included after the fixed portion of the Binding Request option specified above. The presence of such extensions will be indicated by the Option Length field. When the Option Length is greater than 0 octets, the remaining octets are interpreted as extensions. Currently, no extensions have been defined.

4.4. Home Address Option

The Home Address destination option is used in a packet sent by a mobile node to inform the recipient of that packet of the mobile node's home address. For packets sent by a mobile node while away from home, the mobile node generally uses one of its care-of addresses as the Source Address in the packet's IPv6 header. By including a Home Address option in the packet, the correspondent node receiving the packet is able to substitute the mobile node's home address for this care-of address when processing the packet, thus making the use of the care-of address transparent to the correspondent node.

The Home Address option is encoded in type-length-value (TLV) format as follows:



Option Type

195 ???

Option Length

8-bit unsigned integer. Length of the option, in octets, excluding the Option Type and Option Length fields. For the current definition of the Home Address option, this field MUST be set to 8.

Home Address

The home address of the mobile node sending the packet.

The inclusion of a Home Address option in a packet affects only the correspondent node's receipt of this single packet; no state is created or modified in the correspondent node as a result of

receiving a Home Address option in a packet. In particular, the receipt of a packet containing a Home Address option MUST NOT alter the contents of the receiver's Binding Cache due to the presence of the Home Address option, and the mapping between the home address and care-of address indicated by the Home Address option MUST NOT be used as a basis for routing subsequent packets sent by this receiving node.

No special authentication of the Home Address option is required, except that if the IPv6 header of a packet is covered by authentication, then that authentication MUST also cover the Home Address option. If the packet carries no IP authentication, then the contents of the Home Address option, as well as the Source Address field or any other field in the IPv6 header, may have been forged or altered during transit. Upon receipt of a packet containing a Home Address option, the receiving node replaces the Source Address in the IPv6 header with the Home Address in the Home Address option. By requiring that any authentication of the IPv6 header also cover the Home Address option, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option. Security issues related to the Home Address option are discussed further in Section 11.

The three highest-order bits of the Option Type are encoded to indicate specific processing of the option [5]. For the Home Address option, these three bits are set to 110, indicating that the data within the option cannot change en-route to the packet's final destination, and that any IPv6 node processing this option that does not recognize the Option Type must discard the packet and, only if the packet's Destination Address was not a multicast address, return an ICMP Parameter Problem, Code 2, message to the packet's Source Address.

Extensions to the Home Address option format may be included after the fixed portion of the Home Address option specified above. The presence of such extensions will be indicated by the Option Length field. When the Option Length is greater than 8 octets, the remaining octets are interpreted as extensions. Currently, no extensions have been defined.

5. Requirements for IPv6 Nodes

Mobile IPv6 places some special requirements on the functions provided by different IPv6 nodes. This section summarizes those requirements, identifying the functionality each requirement is intended to support. Further details on this functionality is provided in the following sections.

Since any IPv6 node may at any time be a correspondent node of a mobile node, the following requirements pertain to all IPv6 nodes:

- Every IPv6 node MUST be able to process a Home Address option received in a packet.

- Every IPv6 node SHOULD be able to process a Binding Update option received in a packet, and to return a Binding Acknowledgement option if requested.

- Every IPv6 node SHOULD be able to maintain a Binding Cache of the bindings received in accepted Binding Updates.

In order for a mobile node to operate correctly while away from home, at least one IPv6 router in the mobile node's home subnet must function as a home agent for the mobile node. The following special requirements pertain to all IPv6 routers capable of serving as a home agent:

- Every home agent MUST be able to maintain an entry in its Binding Cache for each mobile node for which it is serving as the home agent. Each such Binding Cache entry records the mobile node's binding with its primary care-of address and is marked as a "home registration".

- Every home agent MUST be able to intercept packets (using proxy Neighbor Discovery) on the local subnet addressed to a mobile node for which it is currently serving as the home agent while that mobile node is away from home.

- Every home agent MUST be able to encapsulate such intercepted packets in order to tunnel them to the primary care-of address for the mobile node indicated in its binding.

- Every home agent MUST be able to return a Binding Acknowledgement in response to a Binding Update received with the Acknowledge (A) bit set.

- Every home agent MUST be able to accept packets addressed to the Home-Agents anycast address for the subnet on which it is serving

as a home agent, and MUST be able to participate in dynamic home agent address discovery.

Finally, the following requirements pertain all IPv6 nodes capable of functioning as mobile nodes:

- Every IPv6 mobile node MUST be able to perform IPv6 decapsulation [4].

- Every IPv6 mobile node MUST support sending Binding Updates, as specified in Sections 8.4, 8.5, and 8.6; and MUST be able to receive and process Binding Acknowledgements, as specified in Section 8.9.

- Every IPv6 mobile node MUST maintain a Binding Update List in which it records the IP address of each other node to which it has sent a Binding Update, for which the Lifetime sent in that binding has not yet expired.

6. Correspondent Node Operation

A correspondent node is any node communicating with a mobile node. The correspondent node, itself, may be fixed or mobile, and may possibly also be functioning as a home agent for Mobile IPv6. The procedures in this section thus apply to all IPv6 nodes.

6.1. Receiving Packets from a Mobile Node

Packets sent by a mobile node while away from home generally include a Home Address option. When a node receives a packet containing a Home Address option, it MUST process the option in a manner consistent with copying the Home Address field from the Home Address option into the IPv6 header, replacing the original value of the Source Address field there. Further processing of the packet (e.g., at the transport layer) thus need not know that the original Source Address was a care-of address, or that the Home Address option was used in the packet. Since the sending mobile node uses its home address at the transport layer when sending such a packet, the use of the care-of address and Home Address option is thus transparent to both the mobile node and the correspondent node above the level of the Home Address option generation and processing.

6.2. Receiving Binding Updates

Upon receiving a Binding Update option in some packet, the receiving node MUST validate the Binding Update according to the following tests:

- The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide sender authentication, integrity protection, and replay protection.

- The Option Length field in the Binding Update option is greater than or equal to the length specified in Section 4.1.

- The Sequence Number field in the Binding Update option is greater than the Sequence Number received in the previous Binding Update for this home address, if any. The Sequence Number comparison is performed modulo 2**16.

- The packet MUST contain a valid Home Address option. The home

address for the binding is specified by the Home Address field of the Home Address option.

Any Binding Update not satisfying all of these tests MUST be silently ignored, although the remainder of the packet (i.e., other options, extension headers, or payload) SHOULD be processed normally according to any procedure defined for that part of the packet.

If the Binding Update is valid according to the tests above, then the Binding Update is processed further as follows:

- If the Destination Address in the packet's IPv6 header is the Home-Agents anycast address for a local subnet and this address is assigned to one of this node's network interfaces, then the mobile node sending this Binding Update is attempting dynamic home agent address discovery. Processing for this type of received Binding Update is described in Section 7.1. (If the Destination Address is not assigned to one of this node's network interfaces, then the packet would have been forwarded as a normal packet and the Binding Update, as a destination option, would not be processed in any way by this node.)

- If the Lifetime specified in the Binding Update is nonzero and the specified Care-of Address is not equal to the home address for the binding, then this is a request to cache a binding for the mobile node. Processing for this type of received Binding Update is described in Section 6.3.

- If the Lifetime specified in the Binding Update is zero or the specified Care-of Address matches the home address for the binding, then this is a request to delete the mobile node's cached binding. Processing for this type of received Binding Update is described in Section 6.4.

6.3. Requests to Cache a Binding

If a node receives a valid Binding Update requesting it to cache a binding for a mobile node, as specified in Section 6.2, then the node MUST examine the Home Registration (H) bit in the Binding Update to determine how to further process the Binding Update. If the Home Registration (H) bit is set, the Binding Update is processed according to the procedure specified in Section 7.2.

If the Home Registration (H) bit is not set, then the receiving node SHOULD create a new entry in its Binding Cache for this mobile node (or update its existing Binding Cache entry for this mobile node, if such an entry already exists). The home address of the mobile node is taken from the Home Address field in the packet's Home Address option. The new Binding Cache entry records the association between this address and the care-of address for the binding, as specified

in either the Care-of Address field of the Binding Update or in the Source Address field in the packet's IPv6 header. Any Binding Cache entry created or updated in response to processing this Binding Update MUST be deleted after the expiration of the Lifetime period specified in the Binding Update.

6.4. Requests to Delete a Binding

If a node receives a valid Binding Update requesting it to delete a cached binding for a mobile node, as specified in Section 6.2, then the node MUST examine the Home Registration (H) bit in the Binding Update to determine how to further process the Binding Update. If the Home Registration (H) bit is set, the Binding Update is processed according to the procedure specified in Section 7.3.

If the Home Registration (H) bit is not set, then the receiving node MUST delete any existing entry in its Binding Cache for this mobile node. The home address of the mobile node is taken from the Home Address field in the packet's Home Address option.

6.5. Sending Binding Acknowledgements

When any node receives a packet containing a Binding Update option in which the Acknowledge (A) bit is set, it SHOULD return a Binding Acknowledgement option acknowledging receipt of the Binding Update. If the node accepts the Binding Update and creates or updates an entry in its Binding Cache for this binding, the Status field in the Binding Acknowledgement MUST be set to a value less than 128; if the node rejects the Binding Update and does not create or update an entry for this binding, the Status field in the Binding Acknowledgement MUST be set to a value greater than or equal to 128. Specific values for the Status field are described in Section 4.2 and in the most recent "Assigned Numbers" [15].

As described in Section 4.2, the packet in which the Binding Acknowledgement is returned MUST include an IPv6 Authentication header [1] in order to protect against forged Binding Acknowledgements, and the packet MUST be sent using a Routing header in the same way as any other packet sent to a mobile node using a care-of address (even if the binding was not accepted), as described in Section 6.8. The packet is routed first to the care-of address contained in the Binding Update being acknowledged, and then to the mobile node's home address. This use of the Routing header ensures that the Binding Acknowledgement will be routed to the current location of the node sending the Binding Update, whether the Binding Update was accepted or rejected.

6.6. Cache Replacement Policy

Any entry in a node's Binding Cache MUST be deleted after the expiration of the Lifetime specified in the Binding Update from which the entry was created or was last updated. Conceptually, a node maintains a separate timer for each entry in its Binding Cache. When creating or updating a Binding Cache entry in response to a received and accepted Binding Update, the node sets the timer for this entry to the specified Lifetime period. When a Binding Cache entry's timer expires, the node deletes the entry.

Each node's Binding Cache will, by necessity, have a finite size. A node MAY use any reasonable local policy for managing the space within its Binding Cache, except that any entry marked as a "home registration" (Section 7.2) MUST NOT be deleted from the cache until the expiration of its lifetime period. When attempting to add a new "home registration" entry in response to a Binding Update with the Home Registration (H) bit set, if insufficient space exists (or can be reclaimed) in the node's Binding Cache, the node MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the sending mobile node, in which the Status field is set to 131 (insufficient resources). When otherwise attempting to add a new entry to its Binding Cache, a node MAY, if needed, choose to drop any entry already in its Binding Cache, other than a "home registration" entry, in order to make space for the new entry. For example, a "least-recently used" (LRU) strategy for cache entry replacement among entries not marked as a "home registration" is likely to work well.

Any binding dropped from a node's Binding Cache due to lack of cache space will be rediscovered and a new cache entry created, if the binding is still in active use by the node for sending packets. If the node sends a packet to a destination for which it has dropped the entry from its Binding Cache, the packet will be routed normally, leading to the mobile node's home subnet. There, the packet will be intercepted by the mobile node's home agent and tunneled to the mobile node's current primary care-of address. As when a Binding Cache entry is initially created, this indirect routing to the mobile node through its home agent will result in the mobile node sending a Binding Update to this sending node when it receives the tunneled packet, allowing it to add an entry again for this destination to its Binding Cache.

6.7. Receiving ICMP Error Messages

When a correspondent node sends a packet to a mobile node, if the correspondent node has a Binding Cache entry for the destination

address of the packet, then the correspondent node uses a Routing

header to deliver the packet to the mobile node through the care-of address in the binding recorded in the Binding Cache entry. Any ICMP error message caused by the packet on its way to the mobile node will be returned normally to the correspondent node.

On the other hand, if the correspondent node has no Binding Cache entry for the mobile node, the packet will be routed to the mobile node's home subnet, where it will be intercepted by the mobile node's home agent, encapsulated, and tunneled to the mobile node's primary care-of address. Any ICMP error message caused by the packet on its way to the mobile node while in the tunnel, will be returned to the mobile node's home agent (the source of the tunnel). By the definition of IPv6 encapsulation [4], this encapsulating node MUST relay certain ICMP error messages back to the original sender of the packet, which in this case is the correspondent node.

Likewise, if a packet for a mobile node arrives at the mobile node's previous default router (e.g., the mobile node moved after the packet was sent), the router will encapsulate and tunnel the packet to the mobile node's new care-of address (if it has a Binding Cache entry for the mobile node). As above, any ICMP error message caused by the packet while in this tunnel will be returned to the previous default router (the source of the tunnel), which MUST relay certain ICMP error messages back to the correspondent node [4].

Thus, in all cases, any meaningful ICMP error messages caused by packets from a correspondent node to a mobile node will be returned to the correspondent node. If the correspondent node receives persistent ICMP Host Unreachable or Network Unreachable error messages after sending packets to a mobile node based on an entry in its Binding Cache, the correspondent node SHOULD delete this Binding Cache entry. If the correspondent node subsequently transmits another packet to the mobile node, the packet will be routed to the mobile node's home subnet, intercepted by the mobile node's home agent, and tunneled to the mobile node's primary care-of address using IPv6 encapsulation. The mobile node will then return a Binding Update to the correspondent node, allowing it to recreate a (correct) Binding Cache entry for the mobile node.

6.8. Sending Packets to a Mobile Node

Before sending any packet, the sending node SHOULD examine its Binding Cache for an entry for the destination address to which the packet is being sent. If the sending node has a Binding Cache entry for this address, the sending node SHOULD use a Routing header to route the packet to this mobile node (the destination node) by way

of the care-of address in the binding recorded in that Binding Cache entry. For example, assuming use of a Type 0 Routing header [5], if no other use of a Routing header is involved in the routing of this packet, the mobile node sets the fields in the packet's IPv6 header and Routing header as follows:

- The Destination Address in the packet's IPv6 header is set to the mobile node's care-of address copied from the Binding Cache entry.

- The Routing header is initialized to contain a single route segment, with an Address of the mobile node's home address (the original destination address to which the packet was being sent).

Following the definition of a Type 0 Routing header [5], this packet will be routed to the mobile node's care-of address, where it will be delivered to the mobile node (the mobile node has associated the care-of address with its network interface). Normal processing of the Routing header by the mobile node will then proceed as follows:

- The mobile node swaps the Destination Address in the packet's IPv6 header and the Address specified in the Routing header. This results in the packet's IP Destination Address being set to the mobile node's home address.

- The mobile node then resubmits the packet to its IPv6 module for further processing. Since the mobile node recognizes its own home address as one if its current IP addresses, the packet is processed further within the mobile node, in the same way then as if the mobile node was at home.

If, instead, the sending node has no Binding Cache entry for the destination address to which the packet is being sent, the sending node simply sends the packet normally, with no Routing header. If the destination node is not a mobile node (or is a mobile node that is currently at home), the packet will be delivered directly to this node and processed normally by it. If, however, the destination node is a mobile node that is currently away from home, the packet will be intercepted by the mobile node's home agent and tunneled (using IPv6 encapsulation [4]) to the mobile node's current primary care-of address, as described in Section 7.4. The mobile node will then send a Binding Update to the sending node, as described in Section 8.5, allowing the sending node to create a Binding Cache entry for its use in sending subsequent packets to this mobile node.

7. Home Agent Operation

7.1. Dynamic Home Agent Address Discovery

If a received Binding Update indicates that the mobile node sending it is attempting dynamic home agent address discovery, as described in Section 6.2, then the receiving node MUST process the Binding Update as specified in this section.

A mobile node attempts dynamic home agent address discovery by sending its "home registration" Binding Update to the Home-Agents anycast address for its home IP subnet (the packet MUST also include a Home Address option, as described in Section 8.4). A home agent receiving such a Binding Update that is serving this subnet (the home agent is configured with this anycast address on one of its network interfaces) MUST reject the Binding Update and SHOULD return a Binding Acknowledgement indicating this rejection and giving its unicast address. The Status field in the Binding Acknowledgement MUST be set to 135 (dynamic home agent address discovery response). The mobile node, upon receiving this Binding Acknowledgement, MAY then resend its Binding Update to the unicast home agent address given in the Acknowledgement.

7.2. Primary Care-of Address Registration

General processing of a received Binding Update that requests a binding to be cached, is described in Section 6.3. However, if the Home Registration (H) bit is set in the Binding Update, then the receiving node MUST process the Binding Update as specified in this section, rather than following the general procedure specified in Section 6.3.

To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node is not a router that implements home agent functionality, then the node MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (home registration not supported).

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then the home agent MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home subnet).

- Else, if the home agent chooses to reject the Binding Update for any other reason (e.g., insufficient resources to serve another mobile node as a home agent), then the home agent SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to an appropriate value to indicate the reason for the rejection.

If the home agent does not reject the Binding Update as described above, then it becomes the home agent for the mobile node. The new home agent (the receiving node) MUST then create a new entry or update the existing entry in its Binding Cache for this mobile node's home address, as described in Section 6.3. In addition, the home agent MUST mark this Binding Cache entry as a "home registration"

to indicate that the node is serving as a home agent for this binding. Binding Cache entries marked as a "home registration" MUST be excluded from the normal cache replacement policy used for the Binding Cache (Section 6.6) and MUST NOT be removed from the Binding Cache until the expiration of the Lifetime period.

If the home agent was not already serving as a home agent for this mobile node (the home agent did not already have a Binding Cache entry for this home address marked as a "home registration"), then the home agent MUST multicast onto the home subnet (to the all-nodes multicast address) a Neighbor Advertisement message [9] on behalf of the mobile node, to advertise the home agent's own link-layer address for the mobile node's home IP address. The Target Address in the Neighbor Advertisement message MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the home agent's link-layer address. The Solicited Flag (S) in the Advertisement MUST NOT be set, since it was not solicited by any Neighbor Solicitation message. The Override Flag (O) in the Advertisement MUST be set, indicating that the Advertisement SHOULD override any existing Neighbor Cache entry at any node receiving it.

Any node on the home subnet receiving this Neighbor Advertisement message will thus update its Neighbor Cache to associate the mobile node's home address with the home agent's link layer address, causing it to transmit any future packets for the mobile node instead to the mobile node's home agent. Since multicasts on the local link (such as Ethernet) are typically not guaranteed to be reliable, the home agent MAY retransmit this Neighbor Advertisement message up to MAX_ADVERT_REXMIT times to increase its reliability. It is still possible that some nodes on the home subnet will not receive any of these Neighbor Advertisements, but these nodes will eventually be able to detect the link-layer address change for the mobile node's home address, through use of Neighbor Unreachability Detection [9].

In addition, while this node is serving as a home agent for this mobile node (it still has a "home registration" entry for this mobile node in its Binding Cache), it MUST act as a proxy for this mobile node to reply to any received Neighbor Solicitation messages for it. When a home agent receives a Neighbor Solicitation message, it MUST check if the Target Address specified in the message matches the home address of any mobile node for which it has a Binding Cache entry marked as a "home registration". If such an entry exists in its Binding Cache, the home agent MUST reply to the Neighbor Solicitation message with a Neighbor Advertisement message, giving the home agent's own link-layer address as the link-layer address for the specified Target Address. Likewise, if the mobile node included its home link-local address and set the Home Link-Local Address Present (L) bit in its Binding Update with which it established this "home registration" with its home agent, its home agent MUST also similarly act as a proxy for the mobile node's home link-local address while it has this "home registration" entry in its Binding

Cache. Acting as a proxy in this way allows other nodes on the mobile node's home subnet to resolve the mobile node's IPv6 home address and IPv6 link-local address, and allows the home agent to to defend these addresses on the home subnet for Duplicate Address Detection [9].

7.3. Primary Care-of Address De-registration

General processing of a received Binding Update that requests a binding to be deleted, is described in Section 6.4. However, if the Home Registration (H) bit is set in the Binding Update, then the receiving node MUST process the Binding Update as specified in this section, rather than following the general procedure specified in Section 6.4.

To begin processing the Binding Update, the home agent MUST perform the following sequence of tests:

- If the node is not a router that implements home agent functionality, then the node MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 132 (home registration not supported).

- Else, if the home address for the binding (the Home Address field in the packet's Home Address option) is not an on-link IPv6 address with respect to the home agent's current Prefix List, then it MUST reject the Binding Update and SHOULD return a Binding Acknowledgement to the mobile node, in which the Status field is set to 133 (not home subnet).

If the home agent does not reject the Binding Update as described above, then it MUST delete any existing entry in its Binding Cache for this mobile node.

In addition, in this case, the home agent MUST multicast a Neighbor Advertisement message (to the all-nodes multicast address), giving the mobile node's home address as the Target Address, and specifying the mobile node's link-layer address in a Target Link-layer Address option in the Neighbor Advertisement message. The home agent MAY retransmit this Neighbor Advertisement message up to MAX_ADVERT_REXMIT times to increase its reliability; any nodes on the home subnet that miss all of these Neighbor Advertisements can also eventually detect the link-layer address change for the mobile node's home address, through use of Neighbor Unreachability Detection [9].

7.4. Tunneling Intercepted Packets to a Mobile Node

For any packet sent to a mobile node from the mobile node's home agent (for which the home agent is the original sender of the packet), the home agent is operating as a correspondent node of

the mobile node for this packet and the procedures described in Section 6.8 apply. The home agent (as a correspondent node) uses a Routing header to route the packet to the mobile node by way of the care-of address in the home agent's Binding Cache (the mobile node's primary care-of address, in this case).

In addition, while the mobile node is away from home and this node is acting as the mobile node's home agent, the home agent intercepts any packets on the home subnet addressed to the mobile node's home address, as described in Section 7.2. The home agent cannot use a Routing header to forward these intercepted packets to the mobile node, since it cannot modify the packet in flight without invalidating any existing IPv6 Authentication header present in the packet [1].

For forwarding each intercepted packet to the mobile node, the home agent MUST tunnel the packet to the mobile node using IPv6 encapsulation [4]; the tunnel entry point node is the home agent, and the tunnel exit point node is the mobile node itself (using its primary care-of address as registered with the home agent). When a home agent encapsulates an intercepted packet for forwarding to the mobile node, the home agent sets the Source Address in the prepended tunnel IP header to the home agent's own IP address, and sets the Destination Address in the tunnel IP header to the mobile node's primary care-of address. When received by the mobile node (using its primary care-of address), normal processing of the tunnel header [4]

will result in decapsulation and processing of the original packet by the mobile node.

7.5. Renumbering the Home Subnet

Neighbor Discovery [9] specifies a mechanism by which all nodes on a subnet can gracefully autoconfigure new addresses, say by each node combining a new routing prefix with its existing link-layer address. As currently specified, this mechanism works when the nodes are on the same link as the router issuing the necessary multicast packets to advertise the new routing prefix(es) appropriate for the link.

However, for mobile nodes away from home, special care must be taken to allow the mobile nodes to renumber gracefully. The most direct method of ensuring this is for the home agent to encapsulate and tunnel the multicast packets to the primary care-of address of each mobile node for which it is serving as the home agent. The rules for this are as follows:

- A mobile node assumes that its routing prefix has not changed unless it receives an authenticated Router Advertisement message from its home agent that the prefix has changed.

- When the mobile node is at home, the home agent does not tunnel

Router Advertisements to it.

- The mobile node's home agent serves as a proxy for the mobile node's home address and link-local address, including defending these addresses for Duplicate Address Detection, while the mobile node is registered with the home agent away from home.

- When a home subnet prefix changes, the home agent tunnels Router Advertisement packets to each mobile node registered with it that is currently away from home and using a home address with the affected routing prefix. Such tunneled Router Advertisements MUST be authenticated [1].

- When a mobile node receives a tunneled Router Advertisement containing a new routing prefix, it MUST perform the standard autoconfiguration operation to create its new address.

- When a mobile node returns to its home subnet, it must again perform Duplicate Address Detection at the earliest possible moment after it has deleted its "home registration" binding with its home agent.

- A mobile node MAY send a Router Solicitation to its home agent at any time, within the constraints imposed by rate control defined by Neighbor Discovery [9].

8. Mobile Node Operation

8.1. Sending Packets While Away from Home

While a mobile node is away from home, it continues to use its home address as well as also using one or more care-of addresses. When sending a packet while away from home, a mobile node MAY choose among these in selecting the address that it will use as the source of the packet, as follows:

- For most packets, the mobile node will generally use its home address as the source of the packet. Doing so makes its mobility and the fact that it is currently away from home transparent to the correspondent nodes with which it communicates. For packets sent that are part of transport-level connections established while the mobile node was at home, the mobile node MUST use its home address. Likewise, for packets sent that are part of transport-level connections that the mobile node may still be using after moving to a new location, the mobile node SHOULD use its home address.

- For short-term communication, particularly for communication that may easily be retried if it fails, the mobile node MAY choose to use one of its care-of addresses as the source of the packet. An example of this type of communication might be DNS queries sent by the mobile node [7, 8]. Using the mobile node's care-of address as the source for such queries will generally have a lower overhead than using the mobile node's home address, since no extra options need be used in either the query or its reply, and all packets can be routed normally, directly between their source and destination without relying on Mobile IP. If the mobile node has no particular knowledge that the communication being sent fits within this type of communication, however, the

mobile node SHOULD use its home address.

If the mobile node uses one of its care-of addresses as the source of some packet while away from home, no special Mobile IP processing is required for sending this packet. The packet is simply addressed and transmitted in the same way as any normal IPv6 packet, setting the Source Address field in the packet's IPv6 header to this care-of address.

On the other hand, if the mobile node uses its home address as the source of a packet while away from home, the mobile node SHOULD construct the packet as follows:

- The Source Address field in the packet's IPv6 header is set to one of the mobile node's care-of addresses.

- A Home Address option is included in the packet, with the Home Address field set to the mobile node's home address.

Without this use of the care-of address in the IPv6 header, with the mobile node's home address instead in the Home Address option, the packet will likely be discarded by any router implementing ingress filtering [6].

8.2. Movement Detection

A mobile node MAY use any combination of mechanisms available to it to detect when its link-level point of attachment has moved from one IP subnet to another. The primary movement detection mechanism for Mobile IPv6 defined here uses the facilities of IPv6 Neighbor Discovery, including Router Discovery and Neighbor Unreachability Detection. The description here is based on the conceptual model of the organization and data structures defined by Neighbor Discovery [9].

Mobile nodes SHOULD use Router Discovery to discover new routers and on-link network prefixes; a mobile node MAY send Router Solicitation messages, or MAY wait for unsolicited (periodic) Router Advertisement messages, as specified for Router Discovery [9]. Based on received Router Advertisement messages, a mobile node (in the same way as any other node) maintains an entry in its Default Router List for each router, and an entry in its Prefix List for each network prefix, that it currently considers to be on-link. Each entry in these lists has an associated invalidation timer value (extracted from the Router Advertisement) used to expire the entry when it becomes invalid.

While away from home, a mobile node SHOULD select one router from its Default Router List to use as its default router, and one network prefix advertised by that router from its Prefix List to use as the network prefix in its primary care-of address. A mobile node MAY also have associated additional care-of addresses, using other network prefixes from its Prefix List. The method by which a mobile

node selects and forms a care-of address from the available network prefixes is described in Section 8.3. The mobile node registers its primary care-of address with its home agent, as described in Section 8.4.

While a mobile node is away from home and using some router as its default router, it is important for the mobile node to be able to quickly detect when that router becomes unreachable, so that it can switch to a new default router and to a new primary care-of address. Since some links (notably wireless) do not necessarily work equally well in both directions, it is likewise important for the mobile

node to detect when it becomes unreachable to packets sent from its default router, so that the mobile node can take steps to ensure that any correspondent nodes attempting to communicate with the it can still reach it through some other route.

To detect when its default router becomes unreachable, a mobile node SHOULD use Neighbor Unreachability Detection. As specified in Neighbor Discovery [9], while the mobile node is actively sending packets to (or through) its default router, the mobile node can detect that the router is still reachable either through indications from upper layer protocols on the mobile node that a connection is making "forward progress" (e.g., receipt of TCP acknowledgements for new data transmitted), or through receipt of a Neighbor Advertisement message form its default router in response to an explicit Neighbor Solicitation messages to it. Note that although this mechanism only detects that the mobile node's default router has become unreachable to the mobile node while the mobile node is actively sending packets to it, this is the only time that this direction of reachability confirmation is needed. Confirmation that the mobile node is still reachable from the router is handled separately, as described below.

For a mobile node to detect when it has become unreachable to its default router, however, the mobile node cannot efficiently rely on Neighbor Unreachability Detection alone, since the network overhead would be prohibitively high in many cases for a mobile node to continually probe its default router with Neighbor Solicitation messages even when it is not otherwise actively sending packets to it. Instead, a mobile node SHOULD consider receipt of any IPv6 packets from its current default router as an indication that it is still reachable from the router. Both packets from the router's IP address and (IPv6) packets from its link-layer address (e.g., those forwarded but not originated by the router) SHOULD be considered.

Since the router SHOULD be sending periodic multicast Router Advertisement messages, the mobile node will have frequent opportunity to check if it is still reachable from its default router, even in the absence of other packets to it from the router. On some types of network interfaces, the mobile node MAY also supplement this by setting its network interface into "promiscuous" receive mode, so that it is able to receive all packets on the link, including those not link-level addressed to it. The mobile node will

then be able to detect any packets sent by the router, in order to to detect reachability from the router. This may be useful on very low bandwidth (e.g., wireless) links, but its use MUST be configurable on the mobile node.

If the above means do not provide indication that the mobile node is still reachable from its current default router (i.e., the

mobile node receives no packets from the router for a period of time), then the mobile node SHOULD actively probe the router with Neighbor Solicitation messages, even if it is not otherwise actively sending packets to the router. If it receives a solicited Neighbor Advertisement message in response from the router, then the mobile node can deduce that it is still reachable. It is expected that the mobile node will in most cases be able to determine its reachability from the router by listening for packets from the router as described above, and thus, such extra Neighbor Solicitation probes should rarely be necessary.

With some types of networks, it is possible that additional indications about link-layer mobility can be obtained from lower-layer protocol or device driver software within the mobile node. However, a mobile node MUST NOT assume that all link-layer mobility indications from lower layers indicate a movement of the mobile node's link-layer connection to a new IP subnet, such that the mobile node would need to switch to a new default router and primary care-of address. Upon lower-layer indication of link-layer mobility, the mobile node SHOULD send Router Solicitation messages to determine if new routers (and new on-link network prefixes) are present on its new link.

Such lower-layer information might also be useful to a mobile node in deciding to switch its primary care-of address to one of the other care-of addresses it has formed from the on-link network prefixes currently available through different default routers from which the mobile node is reachable. For example, a mobile node MAY use signal strength or signal quality information (with suitable hysteresis) for its link with the available default routers to decide when to switch to a new primary care-of address using that default router rather than its current default router (and current primary care-of address). Even though the mobile node's current default router may still be reachable in terms of Neighbor Unreachability Detection, the mobile node MAY use such lower-layer information to determine that switching to a new default router would provide a better connection.

8.3. Forming New Care-of Addresses

After detecting that its link-layer point of attachment has moved from one IPv6 subnet to another (i.e., its current default router has become unreachable and it has discovered a new default router), a mobile node SHOULD form a new primary care-of address using one of the on-link network prefixes advertised by the new router. A mobile

node MAY form a new primary care-of address at any time, except that it MUST NOT do so too frequently (not more often than once per MAX_UPDATE_RATE seconds).

In addition, after discovering a new on-link network prefix, a mobile node MAY form a new (non-primary) care-of address using that network prefix, even when it has not switched to a new default router. A mobile node can have only one primary care-of address at a time (which is registered with its home agent), but it MAY have an additional care-of address for any or all of the network prefixes on its current link. Furthermore, since a wireless network interface may actually allow a mobile node to be reachable on more than one link at a time (i.e., within wireless transmitter range of routers on more than one separate link), a mobile node MAY have care-of addresses on more than one link at a time. The use of more than one care-of address at a time is described in Section 8.10.

As described in Section 3.1, in order to form a new care-of address, a mobile node MAY use either stateless [16] or stateful (e.g., DHCPv6 [3]) address autoconfiguration. If a mobile node needs to send packets as part of the method of address autoconfiguration, it MUST use an IPv6 link-local address rather than its own IPv6 home address as the Source Address in the IPv6 header of each such autoconfiguration packet.

In some cases, a mobile node may already know a (constant) IPv6 address that has been assigned to it for its use only while visiting a specific foreign subnet. For example, a mobile node may be statically configured with an IPv6 address assigned by the system administrator of some foreign subnet, for its use while visiting that subnet. If so, rather than using address autoconfiguration to form a new care-of address using this network prefix, the mobile node MAY use its own pre-assigned address as its care-of address on this subnet.

8.4. Sending Binding Updates to the Home Agent

After deciding to change its primary care-of address as described in Sections 8.2 and 8.3, a mobile node MUST register this care-of address with its home agent in order to make this its primary care-of address. To do so, the mobile node sends a packet to its home agent containing a Binding Update option, with the packet constructed as follows:

- The Home Registration (H) bit MUST be set in the Binding Update.
- The Acknowledge (A) bit MUST be set in the Binding Update.
- The packet MUST contain a Home Address option, giving the mobile node's home address for the binding.

- The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, or the Care-of Address Present (C) bit MUST be set in the Binding Update and the care-of address for binding MUST be specified in the Care-of Address field in the Binding Update.

The Acknowledge (A) bit in the Binding Update requests the home agent to return a Binding Acknowledgement in response to this Binding Update. As described in Section 4.2, the mobile node SHOULD retransmit this Binding Update to its home agent until it receives a matching Binding Acknowledgement. Once reaching a retransmission timeout period of MAX_BINDACK_TIMEOUT, the mobile node SHOULD continue to periodically retransmit the Binding Update at this rate until acknowledged (or until it begins attempting to register a different primary care-of address).

It is possible that when the mobile node needs to send such a Binding Update to its home agent, that the mobile node does not know the address of any router in its home subnet that can serve as a home agent for it. In this case, the mobile node SHOULD use the dynamic home agent address resolution procedure to find the address of a suitable home agent in its home subnet. To do so, the mobile node sends the packet, as described above, with the Destination Address in the packet's IPv6 header set the Home-Agents anycast address for its home subnet. The home agent in its home subnet that receives this Binding Update will reject the Update, returning to the mobile node the home agent's unicast IP address. The mobile node SHOULD then retransmit its Binding Update to this home agent using the provided unicast address.

If the mobile node has a current registration with some home agent in its home subnet (the Lifetime for that registration has not yet expired), then the mobile node MUST attempt any new registration first with that home agent. If that registration attempt fails (e.g., times out or is rejected), the mobile node SHOULD then reattempt this registration with another home agent in its home subnet. If the mobile node knows of no other suitable home agent, then it MAY attempt the dynamic home agent address resolution procedure described above.

8.5. Sending Binding Updates to Correspondent Nodes

A mobile node MAY send a Binding Update to any correspondent node at any time to allow it to cache its current care-of address (subject to the rate limiting defined in Section 8.8). In any Binding Update sent by a mobile node, the care-of address (either the Source Address in the packet's IPv6 header or the Care-of Address field in the

Binding Update) MUST be set to one of the care-of addresses currently in use by the mobile node or to the mobile node's home address. If set to one of the mobile node's current care-of addresses (the care-of address given MAY differ from the mobile node's primary care-of address), the Binding Update requests the correspondent node to create or update an entry for the mobile node in the correspondent node's Binding Cache to record this care-of address for use in sending future packets to the mobile node. If, instead, the care-of address is set to the mobile node's home address, the Binding Update requests the correspondent node to delete any existing Binding Cache entry that it has for the mobile node. A mobile node MAY set the care-of address differently for sending Binding Updates to different correspondent nodes.

When sending any Binding Update, the mobile node MUST record in its Binding Update List the following fields from the Binding Update:

- The IP address of the node to which the Binding Update was sent.
- The home address for which the Binding Update was sent,
- The remaining lifetime of the binding, initialized from the Lifetime field sent in the Binding Update.

The mobile node MUST retain in its Binding Update List information about all Binding Updates sent, for which the lifetime of the binding has not yet expired. When sending a Binding Update, if an entry already exists in the mobile node's Binding Update List for an earlier Binding Update sent to that same destination node, the existing Binding Update List entry is updated to reflect the new Binding Update rather than creating a new Binding Update List entry.

In general, when a mobile node sends a Binding Update to its home agent to register a new primary care-of address (as described in Section 8.4), the mobile node will also send a Binding Update to each correspondent node for which an entry exists in the mobile node's Binding Update List. Thus, correspondent nodes are generally kept updated about the mobile node's binding and can send packets directly to the mobile node using the mobile node's current care-of address.

The mobile node, however, need not send these Binding Updates immediately after configuring a new care-of address. For example, since the Binding Update is a destination option and can be included in any packet sent by a mobile node, the mobile node MAY delay sending a new Binding Update to any correspondent node for a short period of time, in hopes that the needed Binding Update can be included in some packet that the mobile node sends to that correspondent node for some other reason (for example, as part of

INTERNET-DRAFT Mobility Support in IPv6 30 July 1997

some TCP connection in use). In this case, when sending a packet

to some correspondent node, the mobile node SHOULD check in its Binding Update List to determine if a new Binding Update to this correspondent node is needed, and SHOULD include the new Binding Update in this packet as necessary.

In addition, when a mobile node receives a packet for which the mobile node can deduce that the original sender of the packet has no Binding Cache entry for the mobile node, or for which the mobile node can deduce that the original sender of the packet has an out-of-date care-of address for the mobile node in its Binding Cache, the mobile node SHOULD return a Binding Update to the sender giving its current care-of address. In particular, the mobile node SHOULD return a Binding Update in response to receiving a packet that meets all of the following tests:

- The packet was tunneled using IPv6 encapsulation.
- The Destination Address in the tunnel (outer) IPv6 header is equal to any of the mobile node's care-of addresses.
- The Destination Address in the original (inner) IPv6 header is equal to the mobile node's home address. If the original packet contains a Routing header, the final Address indicated in the Routing header should be used in this comparison rather than the Destination Address in the original IPv6 header.
- The Source Address in the tunnel (outer) IPv6 header differs from the Source Address in the original (inner) IPv6 header.

The destination address to which the Binding Update should be sent in response to receiving a packet meeting all of the tests above, is the Source Address in the original (inner) IPv6 header of the packet.

Binding Updates sent to correspondent nodes are not generally required to be acknowledged. However, if the mobile node wants to be sure that its new care-of address has been added to a correspondent node's Binding Cache, the mobile node MAY request an acknowledgement by setting the Acknowledge (A) bit in the Binding Update. In this case, however, the mobile node SHOULD NOT continue to retransmit the Binding Update once the retransmission timeout period has reached MAX_BINDACK_TIMEOUT.

A mobile node MAY choose to keep its location private from certain correspondent nodes, and thus need not send new Binding Updates to those correspondents. A mobile node MAY also send a Binding Update to such a correspondent node to instruct it to delete any existing binding for the mobile node from its Binding Cache, as described in

Section 4.1. No other IPv6 nodes are authorized to send Binding Updates on behalf of a mobile node.

8.6. Sending Binding Updates to the Previous Default Router

After switching to a new default router (and thus also changing its primary care-of address), a mobile node SHOULD send a Binding Update to its previous default router, giving its new care-of address. If the mobile node sends such a Binding Update, the home address for the binding, specified in the Home Address option included in the packet carrying this Binding Update, MUST be set the mobile node's old primary care-of address (that it used while using this default router), and the care-of address for the binding (either the Source Address in the packet's IPv6 header or the Care-of Address field in the Binding Update) MUST be set to the mobile node's new primary care-of address. In addition, the Home Registration (H) bit MUST also be set in this Binding Update, to request the mobile node's previous default router to temporarily act as a home agent for the mobile node's old primary care-of address. Note that the previous router does not necessarily know the mobile node's (permanent) home address as part of this registration.

If any subsequent packets arrive at this previous router for forwarding to the mobile node's old primary care-of address, the router SHOULD encapsulate each such packet (using IPv6 encapsulation [4]) and tunnel it to the mobile node at its new primary care-of address. Moreover, for the lifetime of the "home registration" Binding Cache entry for the mobile node at this router, this router MUST act as a proxy for the mobile node's previous care-of address, for purposes of participation in Neighbor Discovery [9], in the same way as any home agent does for a mobile node's home address (Section 7.2). This allows the router to intercept packets addressed to the mobile node's previous care-of address, and to encapsulate and tunnel them to the mobile node's new care-of address, as described in Section 7.4.

8.7. Retransmitting Binding Updates

If, after sending a Binding Update in which the Acknowledge (A) bit is set, a mobile node fails to receive a Binding Acknowledgement within INITIAL_BINDACK_TIMEOUT seconds, the mobile node SHOULD retransmit the Binding Update until a Binding Acknowledgement is received. Such a retransmitted Binding Update MUST use he same Sequence Number value as the original transmission. The retransmissions by the mobile node MUST use an exponential back-off process, in which the timeout period is doubled

upon each retransmission until either the node receives a Binding Acknowledgement or the timeout period reaches the value MAX_BINDACK_TIMEOUT.

8.8. Rate Limiting for Sending Binding Updates

A mobile node MUST NOT send Binding Updates more often than once per MAX_UPDATE_RATE seconds to any node. After sending MAX_FAST_UPDATES

consecutive Binding Updates to a particular node with the same care-of address, the mobile node SHOULD reduce its rate of sending Binding Updates to that node, to the rate of SLOW_UPDATE_RATE per second. The mobile node MAY continue to send Binding Updates at the slower rate indefinitely, in hopes that the node will eventually be able to process a Binding Update and begin to route its packets directly to the mobile node at its new care-of address.

8.9. Receiving Binding Acknowledgements

Upon receiving a packet carrying a Binding Acknowledgement, a mobile node MUST validate the packet according to the following tests:

- The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide both sender authentication, integrity protection, and replay protection.

- The Option Length field in the option is greater than or equal to 9 octets.

- The Sequence Number field matches the Sequence Number sent by the mobile node to this destination address in an outstanding Binding Update.

Any Binding Acknowledgement not satisfying all of these tests MUST be silently ignored, although the remainder of the packet (i.e., other options, extension headers, or payload) SHOULD be processed normally according to any procedure defined for that part of the packet.

When a mobile node receives a packet carrying a valid Binding Acknowledgement, the mobile node MUST examine the Status field as follows:

- If the Status field indicates that the Binding Update was accepted (the Status field is less than 128), then the mobile node MUST update the corresponding entry in its Binding Update

List to indicate that the Binding Update has been acknowledged. The mobile node MUST thus stop retransmitting the Binding Update.

- If the Status field indicates that the Binding Update was not accepted (the Status field is greater than or equal to 128), then the mobile node MUST delete the corresponding Binding Update List entry (and MUST also stop retransmitting the Binding Update). Optionally, the mobile node MAY then take steps to correct the cause of the error and retransmit the Binding Update (with a new Sequence Number value), subject to the rate limiting restriction specified in Section 8.8.

8.10. Using Multiple Care-of Addresses

As described in Section 8.3, a mobile node MAY have more than one care-of address at a time. Particularly in the case of many wireless networks, a mobile node effectively might be reachable through multiple link-level points of attachment at the same time (e.g., with overlapping wireless cells), on which different on-link network prefixes may exist. A mobile node SHOULD select a primary care-of address from among those care-of addresses it has formed using any of these network prefixes, based on the movement detection mechanism in use, as described in Section 8.2. When the mobile node selects a new primary care-of address, it MUST register it with its home agent through a Binding Update with the Home Registration (H) and Acknowledge (A) bits set, as described in Section 8.4.

To assist with smooth handoffs, a mobile node SHOULD retain its previous primary care-of address as a (non-primary) care-of address, and SHOULD still accept packets at this address, even after registering its new primary care-of address with its home agent. This is reasonable, since the mobile node could only receive packets at its previous primary care-of address if it were indeed still connected to that link. If the previous primary care-of address was allocated using stateful address autoconfiguration [3], the mobile node may not wish to release the address immediately upon switching to a new primary care-of address. The stateful address autoconfiguration server will allow mobile nodes to acquire new addresses while still using previously allocated addresses.

8.11. Returning Home

A mobile node detects that it has returned to its home subnet through the movement detection algorithm in use (Section 8.2), when the mobile node detects that the network prefix of its home subnet is again on-link. The mobile node SHOULD then send a Binding Update to

its home agent, to instruct its home agent to no longer intercept or tunnel packets for it. In this Binding Update, the mobile node MUST set the care-of address for the binding (Source Address field in the packet's IPv6 header) to the mobile node's own home address. As with other Binding Updates sent to register with its home agent, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, and SHOULD retransmit the Binding Update until a matching Binding Acknowledgement is received.

In addition, the mobile node MUST multicast onto the home subnet (to the all-nodes multicast address) a Neighbor Advertisement message [9], to advertise the mobile node's own link-layer address for its own home address. The Target Address in this Neighbor Advertisement message MUST be set to the mobile node's home address, and the Advertisement MUST include a Target Link-layer Address option specifying the mobile node's link-layer address. Similarly, the mobile node MUST multicast a Neighbor Advertisement message to

advertise its link-layer address for its IPv6 link-local address. The Solicited Flag (S) in these Advertisements MUST NOT be set, since they were not solicited by any Neighbor Solicitation message. The Override Flag (O) in these Advertisements MUST be set, indicating that the Advertisements SHOULD override any existing Neighbor Cache entries at any node receiving them.

Since multicasts on the local link (such as Ethernet) are typically not guaranteed to be reliable, the mobile node MAY retransmit these Neighbor Advertisement messages up to MAX_ADVERT_REXMIT times to increase their reliability. It is still possible that some nodes on the home subnet will not receive any of these Neighbor Advertisements, but these nodes will eventually be able to recover through use of Neighbor Unreachability Detection [9].

9. Routing Multicast Packets

A mobile node that is connected to its home subnet functions in the same way as any other (stationary) node. Thus, when it is at home, a mobile node functions identically to other multicast senders and receivers. This section therefore describes the behavior of a mobile node that is not on its home subnet.

In order receive packets sent to some multicast group, a mobile node must join the that multicast group. One method by which a mobile node MAY join the group is via a (local) multicast router on the foreign subnet being visited. This option assumes that there is a multicast router present on the foreign subnet. The mobile node SHOULD use its care-of address sharing a network prefix with the multicast router, as the source IPv6 address of its multicast group membership control messages.

Alternatively, a mobile node MAY join multicast groups via a bi-directional tunnel to its home agent, assuming that its home agent is a multicast router. The mobile node tunnels the appropriate multicast group membership control packets to its home agent, and the

home agent forwards multicast packets down the tunnel to the mobile node.

A mobile node that wishes to send packets to a multicast group also has two options: (1) send directly on the foreign subnet being visited; or (2) send via a tunnel to its home agent. Because multicast routing in general depends upon the Source Address used in the IPv6 header of the multicast packet, a mobile node that sends multicast packets directly on the foreign subnet MUST use its care-of address as the IPv6 Source Address of each multicast packet. Similarly, a mobile node that tunnels a multicast packet to its home agent MUST use its home address as the IPv6 Source Address of the inner multicast packet. This second option assumes that the home agent is a multicast router.

10. Constants

INITIAL_BINDACK_TIMEOUT	1 second
MAX_BINDACK_TIMEOUT	256 seconds
MAX_UPDATE_RATE	once per second
SLOW_UPDATE_RATE	once per 10 seconds
MAX_FAST_UPDATES	5
MAX_ADVERT_REXMIT	3

11. Security Considerations

11.1. Binding Updates, Acknowledgements, and Requests

The Binding Update option described in this document will result in packets addressed to a mobile node being delivered instead to its care-of address. This ability to change the routing of these packets could be a significant vulnerability if any packet containing a Binding Update option was not authenticated. Such use of "remote redirection", for instance as performed by the Binding Update option, is widely understood to be a security problem in the current Internet if not authenticated [2].

The Binding Acknowledgement option also requires authentication, since, for example, an attacker could otherwise trick a mobile node into believing a different outcome from a registration attempt with its home agent.

No authentication is required for the Binding Request option, since the use of this option does not modify or create any state in either the sender or the receiver. This Option Does open some issues with binding privacy, but those issues can be dealt with either through existing IPsec encryption mechanisms or through use of firewalls.

The existing IPsec replay protection mechanisms allow a "replay protection window" to support receiving packets out of order. Although appropriate for many forms of communication, Binding Updates MUST be applied only in the order sent. The Binding Update option thus includes a Sequence Number field to provide this necessary

sequencing. The use of this Sequence Number together with IPsec replay protection is similar in many ways, for example, to the the sequence number in TCP. IPsec provides strong replay protection but no ordering, and the sequence number provides ordering but need not worry about replay protection such as through the sequence number wrapping around.

11.2. Home Address Options

No special authentication of the Home Address option is required, except that if the IPv6 header of a packet is covered by authentication, then that authentication MUST also cover the Home Address option. Thus, even when authentication is used in the IPv6 header, the security of the Source Address field in the IPv6 header is not compromised by the presence of a Home Address option. Without authentication of the packet, then any field in the IPv6 header, including the Source Address field, and any other parts of the packet, including the Home Address option, can be forged or modified

in transit. In this case, the contents of the Home Address option is no more suspect than any other part of the packet.

The use of the Home Address option allows packets sent by a mobile node to pass normally through routers implementing ingress filtering [6]. Since the care-of address used in Source Address field of the packet's IPv6 header is topologically correct for the sending location of the mobile node, ingress filtering can trace the location of the mobile node in the same way as can be done with any sender when ingress filtering is in use.

However, if a node receiving a packet that includes a Home Address option implements the processing of this option by physically copying the Home Address field from the option into the IPv6 header, replacing the Source Address field there, then the ability to trace the true location of the sender is removed once this step in the processing is performed. This diminishing of the power of ingress filtering only occurs once the packet has been received at its ultimate destination, and does not affect the capability of ingress filtering while the packet is in transit. Furthermore, this diminishing can be entirely eliminated by appropriate implementation techniques in the receiving node. For example, the original contents of the Source Address field (the sending care-of address) could be saved elsewhere in memory with the packet, until all processing of the packet is completed.

11.3. General Mobile Computing Issues

The mobile computing environment is potentially very different from the ordinary computing environment. In many cases, mobile computers will be connected to the network via wireless links. Such links are particularly vulnerable to passive eavesdropping, active replay

attacks, and other active attacks. Furthermore, mobile computers are more susceptible to loss or theft than stationary computers. Any secrets such as authentication or encryption keys stored on the mobile computer are thus subject to compromise in ways generally not common in the non-mobile environment.

Users who have sensitive data that they do not wish others to see should use mechanisms outside the scope of this document (such as encryption) to provide appropriate protection. Users concerned about traffic analysis should consider appropriate use of link encryption. If stronger location privacy is desired, the mobile node can create a tunnel to its home agent. Then, packets destined for correspondent nodes will appear to emanate from the home subnet, and it may be more difficult to pinpoint the location of the mobile node. Such mechanisms are all beyond the scope of this document.

Appendix A. Changes from Previous Draft

This appendix briefly lists some of the major changes in this draft relative to the previous version of this same draft, draft-ietf-mobileip-ipv6-02.txt:

- Added a comparison to Mobile IP for IPv4 and added this section listing changes from the previous version of this draft.

- Introduced the Home Address destination option, to allow packets sent by a mobile node while away from home to pass normally through routers implementing ingress filtering.

- Added the requirement that all IPv6 nodes MUST be able to correctly process a Home Address destination option in a received packet.

- Changed the interpretation of the Binding Update option such that the home address in the binding is the address in the Home Address option, not the Source Address in the IPv6 header.

- Made the Care-of Address field in the Binding Update optional, controlled by whether or not the new Care-of Address Present (C) bit is set in the option. With the new use of the Home Address option, the care-of address for a binding will usually be specified by the Source Address field in the packet's IPv6 header, but by retaining this field (and making it optional), it is possible to send a binding update using a Source Address different from the care-of address for the binding.

- Changed the 32-bit Identification field in the Binding Update and Binding Acknowledgement to a 16-bit Sequence Number field, and clarified the use of this field. Replay protection for Binding Updates and Binding Acknowledgements is provided by the IPsec authentication in the packet, but this replay protection does not provide sequencing due to the use of the replay protection window. This field satisfies that the additional sequencing

requirement.

- Added a description of the dynamic home agent address discovery procedure and the use of the new Home-Agents anycast address.

Acknowledgements

We would like to thank the members of the Mobile IP and IPng Working Groups for their comments and suggestions on this work. We would particularly like to thank Thomas Narten and Erik Nordmark for their detailed reviews of earlier versions of this draft. Their suggestions have helped to improve both the design and presentation of the protocol.

References

[1] Randall Atkinson. IP Authentication header. RFC 1826, August 1995.

[2] S. M. Bellovin. Security problems in the TCP/IP protocol suite. ACM Computer Communications Review, 19(2), March 1989.

[3] Jim Bound and Charles Perkins. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Internet-Draft, draft-ietf-dhc-dhcpv6-10.txt, May 1997. Work in progress.

[4] Alex Conta and Stephen Deering. Generic packet tunneling in IPv6 specification. Internet-Draft, draft-ietf-ipngwg-ipv6-tunnel-07.txt, December 1996. Work in progress.

[5] Stephen E. Deering and Robert M. Hinden. Internet Protocol version 6 (IPv6) specification. RFC 1883, December 1995.

[6] Paul Ferguson, editor. Network ingress filtering: Defeating IP source address spoofing denial of service attacks. Internet-Draft, draft-ferguson-ingress-filtering-02.txt, July 1997. Work in progress.

[7] P. Mockapetris. Domain Names---concepts and facilities. RFC 1034, November 1987.

[8] P. Mockapetris. Domain Names---implementation and specification. RFC 1035, November 1987.

[9] Thomas Narten, Erik Nordmark, and William Allen Simpson. Neighbor Discovery for IP version 6 (IPv6). RFC 1970, August 1996.

[10] Charles Perkins. IP encapsulation within IP. RFC 2003, October 1996.

[11] Charles Perkins, editor. IP mobility support. RFC 2002, October 1996.

[12] Charles Perkins. Minimal encapsulation within IP. RFC 2004, October 1996.

[13] J. B. Postel. User Datagram Protocol. RFC 768, August 1980.

[14] J. B. Postel, editor. Transmission Control Protocol. RFC 793, September 1981.

[15] Joyce K. Reynolds and Jon Postel. Assigned numbers. RFC 1700, October 1994.

[16] Susan Thomson and Thomas Narten. IPv6 stateless address autoconfiguration. RFC 1971, August 1996.

Chair's Address

The Working Group can be contacted via its current chairs:

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd.
Schaumburg, IL 60196
USA

Phone: +1 847 576-2753
E-mail: solomon@comm.mot.com

Erik Nordmark
Sun Microsystems, Inc.
2550 Garcia Avenue
Mt. View, CA 94041
USA

Phone: +1 415 786-5166
Fax: +1 415 786-5896
E-mail: nordmark@sun.com

Authors' Addresses

Questions about this document can also be directed to the authors:

David B. Johnson
Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213-3891
USA

Phone: +1 412 268-7399
Fax: +1 412 268-5576
E-mail: dbj@cs.cmu.edu

Charles Perkins
Sun Microsystems, Inc.
Technology Development Group
Mail Stop MPK15-214
Room 2682
901 San Antonio Road
Palo Alto, CA 94303
USA

Phone: +1 415 786-6464
Fax: +1 415 786-6445
E-mail: cperkins@eng.sun.com